Nota de prensa

El “QRishing” o el “typosquatting” son algunos de los fenómenos a los que se debe prestar atención para no ser víctima de estafas

La Policía Nacional elabora un decálogo para que el “Black Friday” no se convierta en un “Bad Friday” para tu bolsillo

- **Las redes sociales en ocasiones se pueden convertir en fuente de entrada para la difusión de estafas y, en estos casos, los ciberdelincuentes las utilizan para ofertar artículos llamativos que no existen o para redirigir a páginas fraudulentas**

- **Hay que ser precavidos ante ofertas de artículos populares con grandes descuentos, ya que los estafadores suelen crear sitios falsos de comercio electrónico que desaparecen después de recaudar el dinero de sus víctimas**

- **Los expertos de la Unidad de Ciberdelincuencia advierten sobre los peligros del “typosquatting” -entrar en una página web maliciosa que tiene una dirección muy similar, pero no igual a la del sitio verdadero- o el “QRishing -la manipulación de códigos QR para que la descarga de software malicioso-**

21-noviembre-2023.- Ante el previsible aumento de compras de cara al Black Friday y el Cyber Monday, expertos de la Policía Nacional han elaborado un decálogo para evitar posibles fraudes que se pueden producir en los próximos días. Las redes sociales en ocasiones se han convertido en fuente de entrada para la difusión de estafas, los ciberdelincuentes las pueden utilizar para ofertar artículos llamativos que no existen o para redirigir a páginas fraudulentas

Sigue estos diez consejos para que tu "Black Friday" no se convierta en un "Bad Friday":

1.- ¡Cuidado con algunas promociones que llegan por email o redes sociales! Estos pueden incluir un enlace que te redirige a un sitio web fraudulento donde intentan robar tu información personal y financiera. No pinches ese enlace, busca la oferta en el comercio a través de tu navegador

2.- Gancho: artículos populares con excesivos descuentos. Los estafadores suelen crear sitios falsos de comercio electrónico que desaparecen después de recaudar el dinero de sus víctimas.

3.- No seas víctima de de "typosquatting" (un usuario acaba en una página web que no es la que estaba buscando por teclear mal la URL) Cuando entres en una página verifica que esté bien escrito el nombre en la URL

4.- Atento al "QRishing" los estafadores son capaces de manipular un código QR para que te descargues un software malicioso para infectar tu dispositivo, para hacerse con tus datos más sensibles redirigiéndote a una web fraudulenta

5.- Estos días de tantos envíos es probable que recibas un sms o email de supuestas empresas de paquetería ¡No pinches en los enlaces! ¡Puede ser phishing!

6.- Fíjate en el diseño de la tienda online, imágenes de mala calidad, textos mal traducidos, o faltas de ortografía, que no incluyan CIF, domicilio fiscal,… deben hacer saltar tus alertas

7.- Que el descuento sea en el precio y no en la calidad. Debe mantenerse la misma calidad y derechos

8.- Busca el icono del candado y la "s" en la URL en tu navegador. Esto te dará indicios de que estás ante una página segura

9.- Si la web ya te resulta sospechosa y únicamente te piden datos de tu tarjeta o tu cuenta bancaria ¡Desconfía!

10.- Si has sido víctima de un fraude, cambia contraseñas, cancela la tarjeta de crédito o débito de inmediato, habla con tu banco y denuncia en la Policía Nacional